Managing Security and Resilience in Convergent World

Policy, Operational, and Cultural Considerations

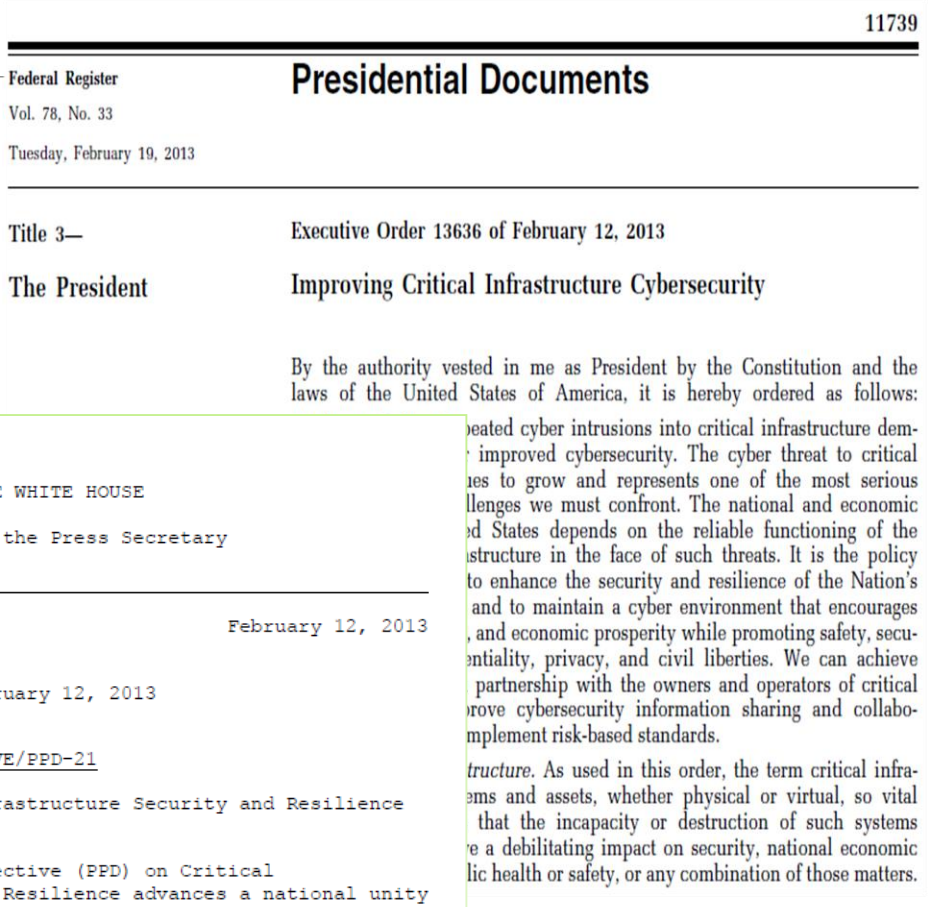
“America must also face the rapidly growing threat from cyber-attacks.”

It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. – PPD 21

"We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.”

Policy Considerations

- Partnerships
- Information Sharing
- Strengthening Capabilities to Reduce and Manage Risk
- Regulatory Requirements



11739

Federal Register
Vol. 78, No. 33
Tuesday, February 19, 2013

Presidential Documents

Title 3—
The President

Executive Order 13636 of February 12, 2013

Improving Critical Infrastructure Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

peated cyber intrusions into critical infrastructure dem-
improved cybersecurity. The cyber threat to critical
ues to grow and represents one of the most serious
llenges we must confront. The national and economic
d States depends on the reliable functioning of the
structure in the face of such threats. It is the policy
to enhance the security and resilience of the Nation's
and to maintain a cyber environment that encourages
, and economic prosperity while promoting safety, secu-
ntiality, privacy, and civil liberties. We can achieve
partnership with the owners and operators of critical
rove cybersecurity information sharing and collabo-
mplement risk-based standards.

tructure. As used in this order, the term critical infra-
ems and assets, whether physical or virtual, so vital
that the incapacity or destruction of such systems
e a debilitating impact on security, national economic
lic health or safety, or any combination of those matters.

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release February 12, 2013

February 12, 2013

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

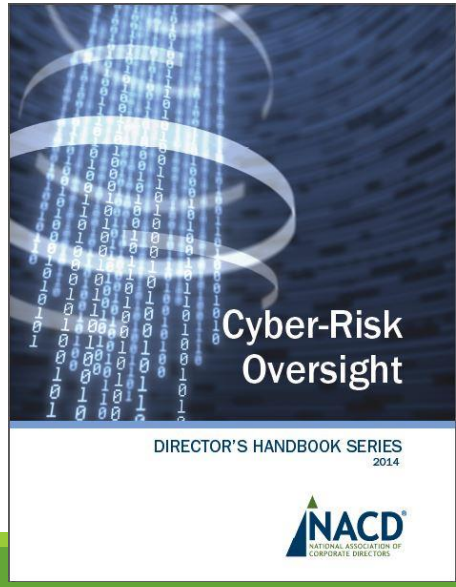
The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Introduction

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-

Operational Considerations

- Changing roles of stakeholders
- Ownership and responsibility
  - Clearly defined
  - Consistent understanding given the different perspectives of stakeholders
- Engaging corporate governance
- Increased CEO and Board engagement
  - http://www.nacdonline.org/cyber
- Interdependencies



Cultural Considerations

- Stakeholders with different perspectives, drivers, and priorities
  - Internal to organization
  - External entities or groups
- Communication and engagement important to understand different perspectives
- Takes time, requires relationship building and trust
- May require executive direction

Holistic Approach Needed

- Policy, operational, and cultural aspects are related
- Some examples:
  - Direction and tone from executives necessary to effectively manage cultural changes
  - Vendors are important stakeholders in policy discussions
  - Security and resilience expectations should be addressed with vendors and third party service providers

Questions?